

## PATENT ABSTRACTS OF JAPAN

G 7 3 9

(11)Publication number : 2001-331375

(43)Date of publication of application : 30.11.2001

(51)Int.Cl.

G06F 12/14  
 G06F 3/06  
 G06F 3/08  
 G06F 9/445  
 G06F 1/00  
 G06F 12/00  
 G06K 19/10  
 G06K 19/00  
 H04L 9/32

(21)Application number : 2000-151808

(71)Applicant : NIPPON LSI CARD CO LTD

(22)Date of filing : 23.05.2000

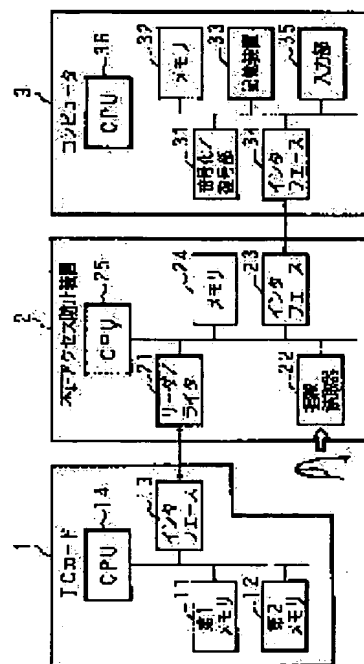
(72)Inventor : OKI SHINJI

(54) PROGRAM STARTUP METHOD, METHOD AND DEVICE FOR PREVENTING  
 UNAUTHORIZED ACCESS, ENCODING/DECODING SYSTEM AND CARD

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a method and a device, capable of preventing an unauthorized user from accessing a storage device in which data is stored at an encoded state by pretending to be someone else.

SOLUTION: Fingerprints of a user to access the storage device 33 in a computer 3 are read by a fingerprint reader 22, data about prescribed fingerprint information stored in a first memory 11 of an IC card 1 are collated with the read fingerprint information, operation algorithm for encoding/decoding stored in a memory 32 is started, only when both pieces of fingerprint information match each other, the data to be stored in the storage device 33 is encoded by an encoding/decoding part 31 and encoded data stored in the storage device 33 is decoded simultaneously.



## LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2001-331375

(P2001-331375A)

(43) 公開日 平成13年11月30日 (2001.11.30)

(51) Int.Cl. <sup>7</sup>	識別記号	F I	テームコード* (参考)
G 0 6 F 12/14	3 2 0	G 0 6 F 12/14	3 2 0 B 5 B 0 1 7
3/06	3 0 4	3/06	3 0 4 H 5 B 0 3 5
3/08		3/08	C 5 B 0 6 5
9/445		12/00	5 3 7 D 5 B 0 7 6
1/00		9/06	6 5 0 D 5 B 0 8 2

審査請求 未請求 請求項の数 8 O L (全 9 頁) 最終頁に続く

(21) 出願番号 特願2000-151808 (P2000-151808)

(22) 出願日 平成12年5月23日 (2000.5.23)

(71) 出願人 000228132

日本エルエスアイカード株式会社

大阪市浪速区日本橋5丁目1番19号

(72) 発明者 大木 信二

大阪府松原市南新町1丁目12番25-609号

(74) 代理人 100078868

弁理士 河野 登夫

Fターム(参考) 5B017 AA07 BA07 BA09 CA07 CA14

5B035 AA14 BB09 BC01

5B065 BA01 BA09 CA40 PA16

5B076 FB05

5B082 EA11 GA11

5J104 AA07 KA01 KA16 KA17 NA33

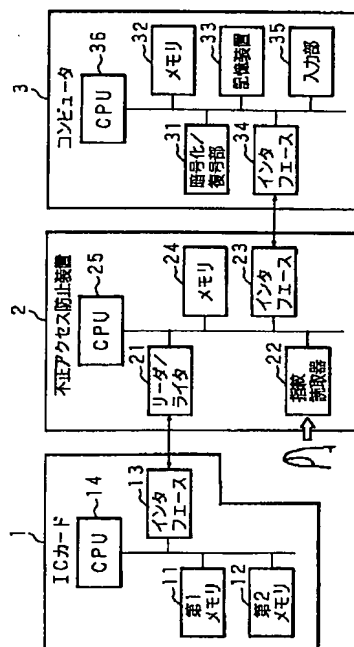
NA38

(54) 【発明の名称】 プログラム起動方法、不正アクセス防止方法及び装置、暗号化／復号システム並びにカード

(57) 【要約】

【課題】 不正なユーザが他人になりすまして、暗号化した状態でデータが記憶される記憶装置へアクセスすることを防止できる方法及び装置を提供する。

【解決手段】 コンピュータ3内の記憶装置33にアクセスするユーザの指紋を指紋読取器22にて読み取り、ICカード1の第1メモリ11に格納されている所定の指紋情報のデータとその読み取った指紋情報とを照合し、一致した場合にのみ、メモリ32に格納されている暗号化用／復号用の動作アルゴリズムが起動されて、暗号化／復号部31にて記憶装置33に記憶すべきデータを暗号化すると共に記憶装置33に記憶されている暗号化データを復号する。



## 【特許請求の範囲】

【請求項 1】 データを暗号化する動作プログラム、及び／または、暗号化されたデータを復号する動作プログラムを、所定の暗証にて起動する方法において、前記暗証として身体的特徴を用いることを特徴とするプログラム起動方法。

【請求項 2】 前記身体的特徴は指紋である請求項 1 記載のプログラム起動方法。

【請求項 3】 暗号化した状態でデータを記憶する記憶装置に対する不正なユーザのアクセスを防止する方法において、前記記憶装置にアクセスしたユーザの身体的特徴を得る第 1 ステップと、得た身体的特徴と所定の身体的特徴とを照合する第 2 ステップと、前記両身体的特徴が一致した場合に、前記記憶装置に記憶すべきデータを暗号化する動作プログラム、及び／または、前記記憶装置に記憶されている暗号化データを復号する動作プログラムを実行する第 3 ステップとを有することを特徴とする不正アクセス防止方法。

【請求項 4】 前記所定の身体的特徴はカードに書き込まれており、前記第 2 ステップにおいて、前記カードから前記所定の身体的特徴を読み出し、読み出した前記所定の身体的特徴と前記第 1 ステップで得た身体的特徴とを照合する請求項 3 記載の不正アクセス防止方法。

【請求項 5】 暗号化した状態でデータを記憶する記憶装置に対する不正なユーザのアクセスを防止する装置において、前記記憶装置にアクセスしたユーザの身体的特徴を取得する取得手段と、取得した身体的特徴と所定の身体的特徴とを照合する照合手段と、前記両身体的特徴が一致した場合に、前記記憶装置に記憶すべきデータを暗号化する動作プログラム、及び／または、前記記憶装置に記憶されている暗号化データを復号する動作プログラムの実行を許可する許可手段とを備えることを特徴とする不正アクセス防止装置。

【請求項 6】 前記取得手段の故障を検知する検知手段と、前記取得手段が故障した場合に、暗証の入力を受け付ける受付手段とを備え、入力された暗証が所定の暗証に一致する場合に、前記許可手段は、前記暗号化する動作プログラム、及び／または、前記復号する動作プログラムの実行を許可すべくしてある請求項 5 記載の不正アクセス防止装置。

【請求項 7】 暗号化した状態でデータを記憶する記憶装置と、前記記憶装置に記憶すべきデータを暗号化する暗号化手段と、前記記憶装置に記憶されている暗号化データを復号する復号手段と、前記記憶装置にアクセスしたユーザの身体的特徴を取得する取得手段と、取得した身体的特徴と所定の身体的特徴とを照合する照合手段と、前記照合手段での照合によって前記両身体的特徴が一致した場合に、前記暗号化手段及び／または前記復号手段での処理の実行を許可する許可手段とを備えることを特徴とする暗号化／復号システム。

【請求項 8】 請求項 1～4 の何れかに記載の方法に用いられるカードであって、前記所定の身体的特徴が書き込まれていることを特徴とするカード。

## 【発明の詳細な説明】

## 【0001】

【発明の属する技術分野】本発明は、データを暗号化する動作プログラム及び／または暗号化されたデータを復号する動作プログラムの起動を制御するプログラム起動方法、暗号化された状態でデータを記憶する記憶装置に対する不正なユーザのアクセスを防止する方法・装置及び暗号化／復号システム、並びに、これらの方法に使用するカードに関する。

## 【0002】

【従来の技術】コンピュータは、ノート型コンピュータに代表されるように、小型化及び可搬化が進んでいる。このような小型のコンピュータにあっても、小型で大容量のハードディスクの搭載により、大量のデータを内部に記憶することができる。また、そのデータを記憶しておくハードディスクにあっては、既存の固定型のものから、高密度実装技術の発展に伴って今後はカード形式の可搬型のものの開発も進行している。

【0003】このような各デバイスの小型化、軽量化が図られていく状況にあって、ノート型コンピュータ本体または可搬型ハードディスクが盗難されて、ハードディスクに記憶されているデータが漏洩または改竄される事態を防止することは重要な問題である。そこで、データをそのままハードディスクに記憶しておくのではなく、記憶すべきデータを暗号化した後にハードディスクに記憶することが一般的に行われている。

【0004】データを暗号化する処理、暗号化されたデータを復号する処理は、夫々、既存の暗号化用の動作プログラム、復号用の動作プログラムに従ってソフトウェア的に行われるが、それらの処理が不正なユーザによってなされないように、各動作プログラムの起動には特定の数字、文字等からなる暗証情報の入力が必要としている。つまり、正しい暗証情報が入力された場合にのみ、これらの暗号化用及び／または復号用の動作プログラムが起動して、ハードディスクにアクセスできるようにしており、これによってノート型コンピュータ本体または可搬型ハードディスクが盗難されても、それらへの不正なアクセスを防止して記憶データの漏洩、改竄を防いでいる。

## 【0005】

【発明が解決しようとする課題】しかしながら、上述した従来の方式では、暗号化用及び／または復号用の動作プログラムを起動させるための暗証情報が数字、文字等にて構成されているので、それが漏洩する可能性もあり、漏洩された場合には不正なユーザがその漏洩暗証情報を用いて容易にそれらの動作プログラムを起動してハードディスクにアクセスすることが可能となり、安全性

が十分ではないという問題がある。

【0006】本発明は斯かる事情に鑑みてなされたものであり、取得した身体的特徴と所定の身体的特徴とを照合して一致した場合に、暗号化用の動作プログラム及び／または復号用の動作プログラムを起動することにより、不正なユーザが他人になりすまして不正に暗号化処理及び／または復号処理を行うことを防止できて従来例よりも安全性を高くできるプログラム起動方法を提供することを目的とする。

【0007】本発明の他の目的は、取得した身体的特徴と所定の身体的特徴とを照合して一致した場合に、暗号化用の動作プログラム及び／または復号用の動作プログラムを起動して記憶装置へのアクセスを可能とすることにより、不正なユーザが他人になりすまして不正に記憶装置へアクセスすることを防止できる不正アクセス防止方法及び装置を提供することにある。

【0008】本発明の更に他の目的は、不正なユーザによる暗号化処理及び／または復号処理を防止できる暗号化／復号システムを提供することにある。

【0009】本発明の更に他の目的は、上記のような方法に使用するカードを提供することにある。

【0010】

【課題を解決するための手段】請求項1に係るプログラム起動方法は、データを暗号化する動作プログラム、及び／または、暗号化されたデータを復号する動作プログラムを、所定の暗証にて起動する方法において、前記暗証として身体的特徴を用いることを特徴とする。

【0011】第1発明のプログラム起動方法にあっては、暗号化用の動作プログラム及び／または復号用の動作プログラムを起動するための暗証として身体的特徴を用いる。身体的特徴は各ユーザにおいて固有のものであるので、他人になりすますことは不可能であり、安全性は極めて強固となる。

【0012】請求項2に係るプログラム起動方法は、請求項1において、前記身体的特徴は指紋であることを特徴とする。

【0013】第2発明のプログラム起動方法にあっては、身体的特徴として指紋を使用する。身体的特徴となる指紋の取得は容易であって本発明の方法を簡便に行えたと共に、指紋は完全に個人を特定できて安全性は極めて高い。

【0014】請求項3に係る不正アクセス防止方法は、暗号化した状態でデータを記憶する記憶装置に対する不正なユーザのアクセスを防止する方法において、前記記憶装置にアクセスしたユーザの身体的特徴を得る第1ステップと、得た身体的特徴と所定の身体的特徴とを照合する第2ステップと、前記両身体的特徴が一致した場合に、前記記憶装置に記憶すべきデータを暗号化する動作プログラム、及び／または、前記記憶装置に記憶されている暗号化データを復号する動作プログラムを実行する

第3ステップとを有することを特徴とする。

【0015】第3発明の不正アクセス防止方法にあっては、記憶装置にアクセスしようとするユーザの身体的特徴を取得し、その身体的特徴が所定の身体的特徴と一致するか否かを判定し、一致した場合にのみ、記憶装置に記憶すべきデータを暗号化する動作プログラム及び／または記憶装置に記憶されている暗号化データを復号する動作プログラムの起動を可能とする。身体的特徴は各ユーザにおいて固有のものであり、不正なユーザが他人になりすまして記憶装置にアクセスすることは不可能であり、記憶装置の安全性は極めて強固となる。

【0016】請求項4に係る不正アクセス防止方法は、請求項3において、前記所定の身体的特徴はカードに書き込まれており、前記第2ステップにおいて、前記カードから前記所定の身体的特徴を読み出し、読み出した前記所定の身体的特徴と前記第1ステップで得た身体的特徴とを照合することを特徴とする。

【0017】第4発明の不正アクセス防止方法にあっては、例えばユーザが携帯するカードに書き込まれている所定の身体的特徴と取得した身体的特徴とを照合する。所定の身体的特徴は、正当なユーザが携帯するカードに書き込まれていて、どこか別のところに格納されていないため、その所定の身体的特徴が漏洩される可能性は非常に低くなり、安全性はより向上する。

【0018】請求項5に係る不正アクセス防止装置は、暗号化した状態でデータを記憶する記憶装置に対する不正なユーザのアクセスを防止する装置において、前記記憶装置にアクセスしたユーザの身体的特徴を取得する取得手段と、取得した身体的特徴と所定の身体的特徴とを照合する照合手段と、前記両身体的特徴が一致した場合に、前記記憶装置に記憶すべきデータを暗号化する動作プログラム、及び／または、前記記憶装置に記憶されている暗号化データを復号する動作プログラムの実行を許可する許可手段とを備えることを特徴とする。

【0019】第5発明の不正アクセス防止装置にあっては、取得手段が記憶装置にアクセスしたユーザの身体的特徴を取得し、照合手段がその取得した身体的特徴と所定の身体的特徴とを照合し、許可手段が、両身体的特徴が一致した場合に、暗号化処理及び／または復号処理を許可する。身体的特徴は各ユーザにおいて固有のものであり、不正なユーザが他人になりすまして記憶装置にアクセスすることは不可能であり、記憶装置に対する不正アクセスを完全に防止する。

【0020】請求項6に係る不正アクセス防止装置は、請求項5において、前記取得手段の故障を検知する検知手段と、前記取得手段が故障した場合に、暗証の入力を受け付ける受付手段とを備え、入力された暗証が所定の暗証に一致する場合に、前記許可手段は、前記暗号化する動作プログラム、及び／または、前記復号する動作プログラムの実行を許可すべくしてあることを特徴とす

る。

【0021】第6発明の不正アクセス防止装置にあっては、検知手段が取得手段の故障を検知し、受付手段が、取得手段が故障した場合に、アクセスしたユーザから暗証の入力を受け付け、許可手段が、入力された暗証が所定の暗証に一致する場合に、暗号化処理及び／または復号処理を許可する。よって、取得手段が故障したときでも、従来例と同様の安全性を維持しながら、正当なユーザが記憶装置へのアクセスを行える。

【0022】請求項7に係る暗号化／復号システムは、暗号化した状態でデータを記憶する記憶装置と、前記記憶装置に記憶すべきデータを暗号化する暗号化手段と、前記記憶装置に記憶されている暗号化データを復号する復号手段と、前記記憶装置にアクセスしたユーザの身体的特徴を取得する取得手段と、取得した身体的特徴と所定の身体的特徴とを照合する照合手段と、前記照合手段での照合によって前記両身体的特徴が一致した場合に、前記暗号化手段及び／または前記復号手段での処理の実行を許可する許可手段とを備えることを特徴とする。

【0023】第7発明の暗号化／復号システムにあっては、取得した身体的特徴と所定の身体的特徴とが一致した場合に、許可手段が、暗号化手段及び／または復号手段での処理の実行を許可する。身体的特徴によって正当なユーザと不当なユーザとが判別され、不正なユーザによる暗号化処理及び／または復号処理は防止される。

【0024】請求項8に係るカードは、請求項1～4の何れかに記載の方法に用いられるカードであって、前記所定の身体的特徴が書き込まれていることを特徴とする。

【0025】第8発明のカードにあっては、そこに正当なユーザ特定するための所定の身体的特徴が書き込まれている。よって、その所定の身体的特徴が漏洩される可能性は非常に低くて安全である。

【0026】

【発明の実施の形態】以下、本発明をその実施の形態を示す図面を参照して具体的に説明する。図1は、本発明における不正アクセス防止方法を利用した暗号化／復号システムの装置構成を示すブロック図である。図1において、1はICカード、2は不正アクセス防止装置、3はコンピュータである。

【0027】ICカード1はこのコンピュータ3を使用するユーザ毎に発行され、各ユーザは自身固有のICカード1を有する。このICカード1は接触または非接触での情報の書込み／読出し処理が可能なカードである。

【0028】ICカード1は、所有するユーザの身体的情報である指紋情報のデータを格納する第1メモリ11と、コンピュータ3でのデータの暗号化／復号処理の動作プログラムの起動に必要な暗証情報のデータを格納する第2メモリ12と、不正アクセス防止装置2（リーダ／ライタ21）との間で情報を送受するインタフェース

13と、これらの各機能素子の動作を制御するCPU14とを有する。ICカード1の発行時に、指紋情報のデータとこれに対となる暗証情報のデータとが、第1メモリ11と第2メモリ12とに夫々書き込まれる。

【0029】不正アクセス防止装置2は、ICカード1に対して情報の書込み／読出し処理を行うリーダ／ライタ21と、ユーザの指紋情報を得る指紋読取器22と、コンピュータ3との間で情報を送受するインタフェース23と、指紋照合処理等の動作プログラム等を格納しているメモリ24と、これらの各機能機器の動作を制御すると共に後述するソフトウェアの処理を実行するCPU25とを有する。リーダ／ライタ21は、ICカード1が装填された場合に、そこに格納されている各種のデータ（指紋情報のデータ、暗証情報のデータ等）を読み出し、指紋情報のデータをCPU25へ与え、暗証情報のデータをインタフェース23を介してコンピュータ3へ出力する。指紋読取器22は、光学的または静電的に指紋を読み取り、読み取った指紋情報をCPU25へ与える。

【0030】上述した第1メモリ11及び第2メモリ12には夫々錠がかけられており、各メモリ11、12から格納データを読み出す際には夫々の錠を鍵で解く必要がある。第1メモリ11に対する鍵は、リーダ／ライタ21が有しており、リーダ／ライタ21に対応する正当なICカード1であることが鍵となって、第1メモリ11は開錠される。また、第2メモリ12に対する鍵は、不正アクセス防止装置2が有しており、ICカード1から読み出された指紋情報の格納データと指紋読取器22にて得られた指紋情報との一致が鍵となって、第2メモリ12は開錠される。

【0031】コンピュータ3は、データを暗号化する暗号化処理及び暗号化データを復号する復号処理を行う暗号化／復号部31と、暗号化用の動作プログラム、復号用の動作プログラム等を格納しているメモリ32と、データを暗号化された状態で記憶する記憶装置33と、不正アクセス防止装置2との間で情報を送受するインタフェース34と、外部入力を受け付ける入力部35と、これらの各機能部の動作を制御するCPU36とを有する。不正アクセス防止装置2からインタフェース34を介して正しい暗証が入力された場合に、メモリ32に格納されている暗号化用／復号用のプログラムが暗号化／復号部31に読み出されて起動し、暗号化処理／復号処理が行われるようになっている。

【0032】次に、本発明における不正アクセス防止方法における動作について、その手順を示す図2～図5のフローチャートを参照して説明する。

【0033】まず、指紋情報及び暗証情報の登録処理について説明する。図2は、その処理の動作手順を示すフローチャートである。このコンピュータ3を使用するユーザの指紋を指紋読取器22にて読み取って指紋情報を

取得し、そのデータをリーダ/ライタ21にてIDカード1の第1メモリ11に書き込んで格納する(ステップS11)。

【0034】この際、CPU25は、制御プログラムによって特定の数字または文字を発生する。このように発生して設定される特定の数字または文字は、そのユーザの指紋情報のデータと対になる暗証情報であり、そのデータをリーダ/ライタ21にてIDカード1の第2メモリ12に書き込んで格納する(ステップS12)。なお、これらの指紋情報のデータ及び暗証情報のデータを暗号化して格納しておくようにした場合には、セキュリティが向上する。

【0035】そして、その暗証情報をコンピュータ3に登録する(ステップS13)。また、これらの指紋情報のデータ及び暗証情報のデータを、そのまま、または暗号化して、緊急復元カードにも書き込んで格納しておく(ステップS14)。この緊急復元カードは、指紋読取器22の故障等によって指紋照合が不可能になった場合のデータ復元の際に利用されるものであり、通常は厳重に保管される。

【0036】なお、指紋情報及び暗証情報の登録処理を図1に示す構成部品を利用して行う場合について説明したが、図1のシステムとは無関係にこのような登録処理を行うようにしても良い。

【0037】次に、データを暗号化して記憶装置33に記憶する暗号化処理について説明する。図3は、その処理の動作手順を示すフローチャートである。コンピュータ3にアクセスしようとするユーザが携帯するIDカード1が、リーダ/ライタ21に装填される(ステップS21)。CPU25は、装填されたIDカード1が、そのリーダ/ライタ21に対応する正規のカードであるかを判断する(ステップS22)。正規のカードである場合に(S22: YES)、第1メモリ11の錠が開けられて、そこに格納されている指紋情報のデータがリーダ/ライタ21にてCPU25に読み出される(ステップS23)。正規のカードでないと判断された場合には(S22: NO)、そのまま動作が終了する。

【0038】指紋読取器22にて、ユーザの指紋を読み取って指紋情報を得る(ステップS24)。CPU25は、得られた指紋情報と、読み出された指紋情報のデータとを照合して、両者が一致するかを判断する(ステップS25)。一致する場合に(S25: YES)、第2メモリ12の錠が開けられて、そこに格納されている暗証情報のデータがリーダ/ライタ21にて読み出される(ステップS26)。一致しないと判断された場合には(S25: NO)、そのまま動作が終了する。

【0039】不正アクセス防止装置2に読み出された暗証情報は、インターフェース23、34を介してコンピュータ3に送られる。これによって、メモリ32から暗号化用の動作プログラムが読み出され、暗号化/復号部

31にてその動作プログラムが起動されて、記憶すべきデータに対する暗号化処理が施される(ステップS27)。そして、暗号化されたデータは、記憶装置33に記憶される(ステップS28)。

【0040】次に、記憶装置33に記憶されている暗号化データを復号する復号処理について説明する。図4は、その処理の動作手順を示すフローチャートである。コンピュータ3にアクセスしようとするユーザが携帯するIDカード1が、リーダ/ライタ21に装填される(ステップS31)。CPU25は、装填されたIDカード1が、そのリーダ/ライタ21に対応する正規のカードであるかを判断する(ステップS32)。正規のカードである場合に(S32: YES)、第1メモリ11の錠が開けられて、そこに格納されている指紋情報のデータがリーダ/ライタ21にてCPU25に読み出される(ステップS33)。正規のカードでないと判断された場合には(S32: NO)、そのまま動作が終了する。

【0041】指紋読取器32にて、ユーザの指紋を読み取って指紋情報を得る(ステップS34)。CPU25は、得られた指紋情報と、読み出された指紋情報のデータとを照合して、両者が一致するかを判断する(ステップS35)。一致する場合に(S35: YES)、第2メモリ12の錠が開けられて、そこに格納されている暗証情報のデータがリーダ/ライタ21にて読み出される(ステップS36)。

【0042】不正アクセス防止装置2に読み出された暗証情報は、インターフェース23、34を介してコンピュータ3に送られる。これによって、メモリ32から復号用の動作プログラムが読み出され、暗号化/復号部31にてその動作プログラムが起動されて、記憶装置33に記憶されている暗号化データに対する復号処理が施される(ステップS37)。そして、復号されたデータが出力される(ステップS38)。

【0043】指紋読取器32で得られた指紋情報とICカード1から読み出された指紋情報のデータとが一致しない場合に(S35: NO)、CPU25は、指紋読取器22が故障しているかを判断する(ステップS39)。故障している場合(S39: YES)、入力部35により暗証情報の外部入力を受け付ける(ステップS40)。これによって、復号用の動作プログラムが起動されて、記憶装置33に記憶されている暗号化データが復号され(S37)、復号されたデータが出力される(S38)。このように、指紋読取器32が故障した場合に、その故障を自身で検知して、暗証情報の外部入力により復号処理を行う補助機能を有している。この際、安全性を確保するために、外部入力された暗証情報がコンピュータ3に残存しないようにする。

【0044】なお、前述した暗号化処理にあっても、指紋情報の一致が見られない場合に、同様に、指紋読取器

22の故障を検知したときに暗証情報の外部入力を受け付けて、データの暗号化を行えるように構成しても良い。

【0045】次に、指紋照合が行えなくなった場合の復元処理について説明する。図5は、その処理の動作手順を示すフローチャートである。緊急復元カードに格納されている暗証情報を読み出し、読み出した暗証情報をコンピュータ3に入力部35を介して入力する(ステップS41)。メモリ32内の復号用の動作プログラムを起動して、記憶装置33に記憶されている全ての暗号化データを暗号化/復号部31にて復号する(ステップS42)。その後、登録されている指紋情報と暗証情報との対を削除する(ステップS43)。よって、例えばユーザの指が損傷して指紋照合が不可能となった場合でも、暗号化データを元のデータに復号することができる。

【0046】以下、本発明の不正アクセス防止装置をコンピュータに内蔵した実施の形態について説明する。図6は、このような簡易型の実施の形態の第1例における可搬型コンピュータの要部構成を示すブロック図である。この可搬型コンピュータ4は、1チップの集積回路で構成された指紋スキャナ41と、データを暗号化する暗号化処理及び暗号化データを復号する復号処理を行う暗号化/復号部42と、暗号化用/復号用の動作プログラム、指紋照合処理の動作プログラム、所定のユーザの指紋情報のデータ等を格納しているメモリ43と、データを暗号化された状態で記憶する記憶装置44と、これらの各機能部の動作を制御すると共に後述するソフトウェアの処理を実行するCPU45とを有する。この例では、以下に述べるように、指紋の照合結果を直接、暗号化用/復号用の動作プログラムを起動するための暗証情報として用いている。

【0047】次に、データを暗号化して記憶装置44に記憶する暗号化処理について説明する。図7は、その処理の動作手順を示すフローチャートである。コンピュータ3にアクセスしようとするユーザの指紋を指紋スキャナ41で読み取って指紋情報を得る(ステップS51)。CPU45は、得られた指紋情報とメモリ43から読み出した所定の指紋情報のデータとを照合して、両者が一致するかどうかを判断する(ステップS52)。一致する場合に(S52: YES)、メモリ43から暗号化用の動作プログラムを読み出され、暗号化/復号部42にてその動作プログラムが起動されて、記憶すべきデータに対する暗号化処理が施される(ステップS53)。そして、暗号化されたデータは、記憶装置44に記憶される(ステップS54)。一方、一致しない場合には(S52: NO)、動作はそのまま終了する。

【0048】次に、記憶装置44に記憶されている暗号化データを復号する復号処理について説明する。図8は、その処理の動作手順を示すフローチャートである。コンピュータ3にアクセスしようとするユーザの指紋を

指紋スキャナ41で読み取って指紋情報を得る(ステップS61)。CPU45は、得られた指紋情報とメモリ43から読み出した所定の指紋情報のデータとを照合して、両者が一致するかどうかを判断する(ステップS62)。一致する場合に(S62: YES)、メモリ43から復号用の動作プログラムを読み出され、暗号化/復号部42にてその動作プログラムが起動されて、記憶装置44に記憶されている暗号化データに対する復号処理が施される(ステップS63)。そして、復号されたデータは出力される(ステップS64)。一方、一致しない場合には(S62: NO)、動作はそのまま終了する。

【0049】図9は、このような簡易型の実施の形態の第2例における可搬型コンピュータの要部構成を示すブロック図である。この可搬型コンピュータ4は、第1例と同様の指紋スキャナ41及び暗号化/復号部42と、データを暗号化された状態で記憶する取外し可能な記憶装置51と、ネットワークとの通信を行う通信部52と、暗号化用/復号用の動作プログラム、指紋照合処理の動作プログラム、通信部52での通信処理用の動作プログラム、所定のユーザの指紋情報のデータ等を格納しているメモリ53と、これらの各機能部の動作を制御すると共に上述したようなソフトウェアの処理を実行するCPU54とを有する。この例では、記憶装置51が、可搬型コンピュータ4に着脱可能なカード型の可搬型記憶装置である。

【0050】この第2例でも、暗号化用/復号用の動作プログラムを起動するための暗証情報として指紋の照合結果を用いており、第2例における暗号化処理/復号処理は第1例の場合と同様である。

【0051】また、第2例では、通信部52での通信処理の実行には、正当なユーザであるかどうかの認証を必要とする。そして、この正当なユーザであるかどうかの判断に、暗号化用/復号用の動作プログラムの起動時と同様に、指紋の照合結果を用いる。

【0052】なお、上述した実施の形態では、身体的特徴として指紋を用いる場合について説明したが、本発明はこれに限らず、掌紋、アイリス、声紋、顔の特徴等、他の身体的特徴を用いることも可能であることは勿論である。

【0053】また、1人のユーザが1台のコンピュータの記憶装置にアクセスできるようにした例について説明したが、本発明はこれに限らず、特定の複数のユーザがアクセスできるようにも構成できることはいうまでもない。

【0054】

【発明の効果】以上のように第1発明のプログラム起動方法では、暗号化用の動作プログラム及び/または復号用の動作プログラムの起動用の暗証として、各ユーザにおいて固有のものである身体的特徴を用いるようにした

ので、他人になりすますことは不可能であり、極めて高い安全性を実現できる。

【0055】第2発明のプログラム起動方法では、身体的特徴として指紋情報を使用するようにしたので、容易に身体的特徴を取得でき、正確かつ簡便に正規のユーザを特定することが可能である。

【0056】第3発明の不正アクセス防止方法では、ユーザの身体的特徴が所定の身体的特徴と一致するか否かを判定し、一致した場合にのみ、記憶装置に記憶すべきデータを暗号化する動作プログラム及び／または記憶装置に記憶されている暗号化データを復号する動作プログラムの起動を可能とするようにしたので、不正なユーザが他人になりすまして記憶装置にアクセスすることは不可能であり、記憶装置へのアクセスに関して極めて高い安全性を実現できる。

【0057】第4発明の不正アクセス防止方法では、カードに書き込まれている所定の身体的特徴と取得した身体的特徴とを照合するようにしたので、その所定の身体的特徴が漏洩される可能性は非常に低くなり、安全性をより向上できる。

【0058】第5発明の不正アクセス防止装置では、取得した身体的特徴と所定の身体的特徴とが一致した場合に、暗号化処理及び／または復号処理を許可するようにしたので、不正なユーザが他人になりすまして記憶装置にアクセスすることは不可能であり、記憶装置に対する不正アクセスを完全に防止することができる。

【0059】第6発明の不正アクセス防止装置では、身体的特徴を取得する取得手段の故障を検知した場合に、暗証の入力を受け付けるようにしたので、取得手段が故障したときでも、従来例と同様の安全性を維持しながら、正当なユーザが記憶装置へのアクセスを行うことができる。

【0060】第7発明の暗号化／復号システムでは、取得した身体的特徴と所定の身体的特徴とが一致した場合に、暗号化手段及び／または復号手段での処理の実行を許可するようにしたので、身体的特徴によって正当なユーザと不当なユーザとを容易に判別でき、不正なユーザによる暗号化処理及び／または復号処理を完全に防止できる。

【0061】第8発明のカードでは、正当なユーザ特定

10

20

30

40

するための所定の身体的特徴が書き込まれるようにしたので、その所定の身体的特徴が漏洩される可能性は非常に低くて安全である。

【図面の簡単な説明】

【図1】本発明における不正アクセス防止方法を利用した暗号化／復号システムの装置構成を示すブロック図である。

【図2】指紋情報及び暗証情報の登録処理の動作手順を示すフローチャートである。

【図3】暗号化処理の動作手順を示すフローチャートである。

【図4】復号処理の動作手順を示すフローチャートである。

【図5】指紋照合が行えなくなった場合の復元処理の動作手順を示すフローチャートである。

【図6】本発明の不正アクセス防止装置をコンピュータに内蔵した第1例の要部構成を示すブロック図である。

【図7】暗号化処理の動作手順を示すフローチャートである。

【図8】復号処理の動作手順を示すフローチャートである。

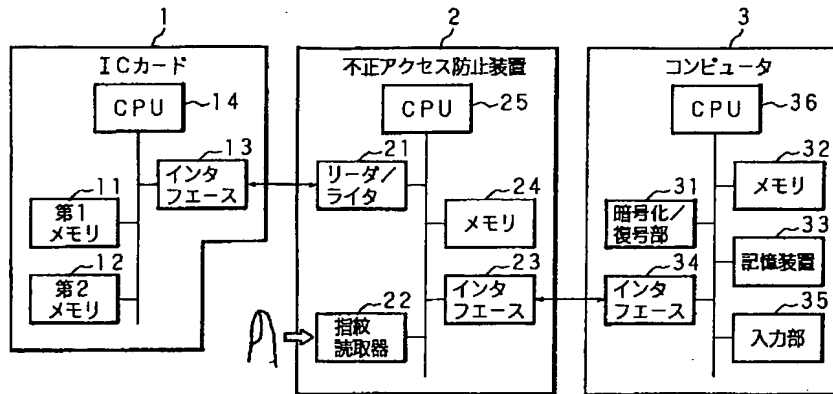
【図9】本発明の不正アクセス防止装置をコンピュータに内蔵した第2例の要部構成を示すブロック図である。

【符号の説明】

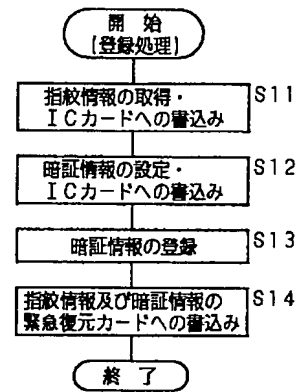
- 1 ICカード
- 2 不正アクセス防止装置
- 3 コンピュータ
- 4 可搬型コンピュータ
- 11 第1メモリ
- 12 第2メモリ
- 14, 25, 36, 45, 54 CPU
- 21 リーダ／ライター
- 22 指紋読取器
- 31, 42 暗号化／復号部
- 24, 32, 43, 53 メモリ
- 33, 44, 51 記憶装置
- 35 入力部
- 41 指紋スキャナ
- 52 通信部



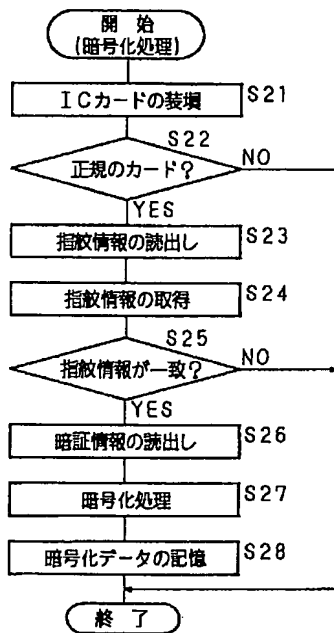
【図1】



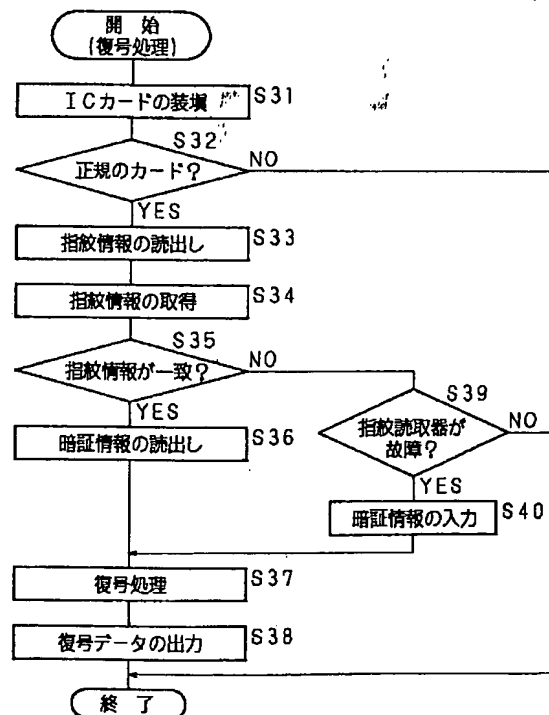
【図2】



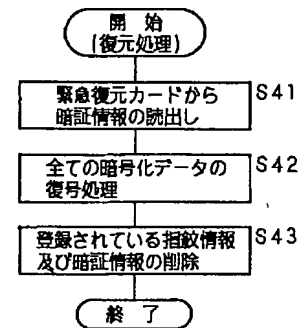
【図3】



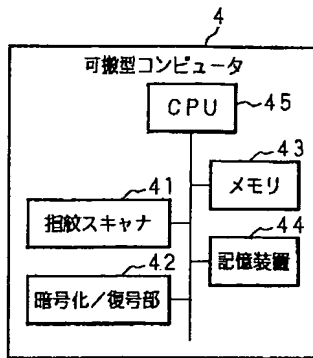
【図4】



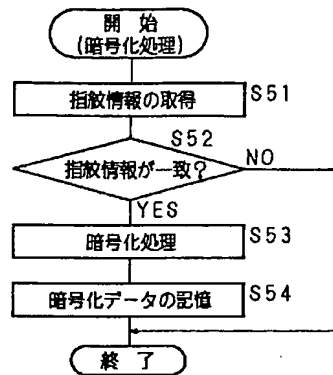
【図5】



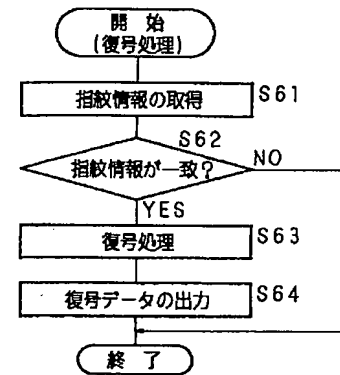
【図6】



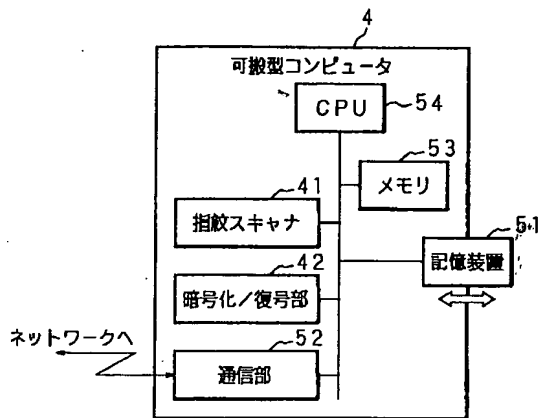
【図7】



【図8】



【図9】



フロントページの続き

(51)Int.Cl.<sup>7</sup>

G 0 6 F 12/00

G 0 6 K 19/10

19/00

H 0 4 L 9/32

識別記号

5 3 7

F I

G 0 6 F 9/06

G 0 6 K 19/00

H 0 4 L 9/00

テーマコード (参考)

6 6 0 E 5 J 1 0 4

S

T

6 7 3 A

6 7 3 D

6 7 3 E